EXHIBIT C

Michael Carter is an expert in regulatory compliance and anti-financial crime programs. He has extensive experience applying his knowledge of risk and compliance matters to businesses in the US and abroad. He regularly advises on financial compliance matters, including but not limited to, issues related to money laundering, sanctions, fraud, consumer protection, data privacy and protection, and market integrity. He also has written and spoken extensively on the topics of risk and compliance.

Mr. Carter is a Certified Anti-Money Laundering Specialist (CAMS), Certified Fraud Examiner (CFE), Certified Global Sanctions Specialist (CGSS), and Project Management Professional (PMP), and possesses the Travel Rule Fundamentals Certification (NB-TRFC). He earned a Bachelor of Arts degree (BA) from the University of North Florida and an Executive Master of Business Administration (EMBA) degree from George Mason University.

He served as the AML/BSA/Sanctions Committee Chair for the Virtual Commodity Association in 2019-2020. Mr. Carter also served on the AML Committee for the TRUST Travel Rule consortium from 2020-2023.

OPINION 1: Neither the decentralized blockchain protocol Tornado Cash, nor the Tornado Cash website and User Interface ("UI") or Command Line Interface ("CLI") possessed formal customer relationships nor did they transfer financial assets or property. This renders them like information sharing intermediaries, not financial institutions or money transmitters.

1. The Financial Crimes Enforcement Network (FinCEN) is a Department of the U.S. Treasury and regulates money transmitters, which are businesses that transfer funds on behalf of the public by any various means including wire. Money transmitters, like traditional financial institutions such as banks, are subject to the Bank Secrecy Act (BSA) and its implementing regulations. The BSA and regulations mandate the application of internal controls, recording, and reporting of financial crime activity by financial institutions and companies that operate as money transmitters. Those regulations do not apply to organizations that merely transmit information.

2. Tornado Cash is computer code that operates independently via smart contracts on the blockchain(s). There is no corporate structure, or employees. Their smart contract code operated independently and autonomously. At no point did Tornado Cash actually take custody of or transfer any funds or property.

3. The developers of Tornado Cash developed and made public immutable smart contracts. These smart contracts executed blockchain transactions without involvement from a Tornado Cash entity or a third party. As a decentralized blockchain protocol, Tornado Cash has functioned as an information sharing intermediary utilizing smart contracts (code) to exchange information. The fact that the Tornado Cash developers also created informational tools such as the website, UI, or CLI to assist users in using the protocol does not change the analysis, as those tools also did not take custody of the funds.

4. Not all organizations that have a role in finance are subject to the BSA regulations. Certain information sharing intermediaries are not, such as the National Automated Clearing House Association (Nacha)[1] and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network.[2]

[1] https://www.nacha.org/
[2] https://www.swift.com/about-us

5. Nacha is a non-profit organization that manages the Automated Clearing House (ACH) network --a US financial network for electronic payments. Although it facilitates electronic payments, at no point does ACH take custody of or transfer funds itself, but serves as an information router for transactions initiated by other parties.[3]

6. SWIFT functions as a global messaging network that allows banks to securely communicate with each other. SWIFT sends electronic instructions for transferring funds between accounts, essentially providing information between banks so that they can conduct transactions. However, at no point does SWIFT actually handle or transfer any funds. Similar to Nacha, SWIFT is neither a financial institution nor a money transmitter.[4]

7. Like Nacha and Swift, neither the Tornado Cash protocol nor the website, UI, or CLI actually transfers any digital assets or property. The protocol never had custody of users' assets, as users move their funds using their own private keys. This meant that the users maintained control over their assets. Further, the UI and CLI that Peppersec created are particularly like SWIFT and Nacha because they do not touch any cryptocurrency or conduct any transactions but are merely an information-sharing resource for users.

OPINION 2: Due to inherent limitations in Know Your Customer (KYC) tools and processes, it was, and continues to be, impossible for Tornado Cash to apply KYC procedures.

8. The government's expert, Phillip Werlau, who has no cited experience in designing and implementing compliance systems, advances the following claims:

    a. Tornado Cash "could also have been changed to implement KYC processes, which would also have the effect of enabling more effective sanctions screening by providing information about who the customer initiating the deposit or withdrawal was. Embedding compliance tools into the architecture in this would have made it more difficult for Tornado Cash customers to evade the minimal sanctions screening embedded into the UI in April 2022." (¶ 19)

    b. "The changes to the Tornado Cash service in February 2022 also demonstrate that the Tornado Cash founders ***could have included a know-your-customer ("KYC") function*** in the Tornado Cash service. . . . ***This hypothetical smart contract*** could have been set up so that the Tornado Cash founders . . . had the ability to add or remove users based on a KYC process." (¶ 18 (emphasis added))

9. While Mr. Werlau does not define KYC processes or function, KYC processes include identity verification and due diligence tools with the intent to provide an organization with an understanding of the nature and purpose of counterparty relationships, while conducting ongoing monitoring to identify and report suspicious transactions.[5] KYC tools may perform various specialized functions that are distinct in nature

[3] https://www.nacha.org/content/legal-information;
Searches conducted:
https://www.fincen.gov/msb-state-selector;
https://www.occ.treas.gov/institution-search/list?q=national%20automated%20clearinghouse

[4] Searches conducted:
https://www.occ.treas.gov/institution-search/list?q=swift;
https://www.fincen.gov/msb-state-selector

[5] https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule

from one another, but generally fall under the umbrella of common KYC activities.[6] Those functions commonly include[7]:

a. Identity Verification

   i. Obtaining the identifying information (including name, date of birth for an individual, address, and identification number).

   ii. Verifying the identity of each customer to the extent reasonable and practicable through risk-based procedures, often including the collection and verification of identification documents.

   iii. While identity verification activities such as ID capture and validation and user photo capture are commonly conducted using third-party automation, there is a material failure rate common among identity verification providers that results in erroneous approvals, fraudulent ID acceptance, or verification processing failures that require manual review and disposition.[8]

b. Customer Due Diligence

   i. Understanding the nature of a customer's business, their financial transactions, and the overall purpose of their relationship with the institution.

   ii. Collecting information regarding a customer's source of funds or source of wealth.

   iii. Conducting name and attribute screening of the customer against sanctions lists, Politically Exposed Persons[9] lists, adverse public information, criminal databases, or other government lists.

   iv. Collecting data regarding IP address usage for web-based customers.

c. Enhanced Due Diligence

   i. Verifying information regarding a customer's stated source of funds or source of wealth, employment through documentation.

   ii. Verifying other customer-provided or third-party information as needed to make informed risk-based decisions about the customer's relationship with the institution.

---

[6] Reference, in part, the Federal Financial Institutions Examination Council BSA/AML Manual: https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/01

[7] Depending on the organization, some KYC activities may overlap or occur at different phases of the customer lifecycle based on their risk-based compliance approach.

[8] Reference: https://network.id.me/inclusion-and-access-research-methodology/; https://network.id.me/article/accelerating-digital-access-the-impact-of-id-mes-identity-wallet/https://www.biometricupdate.com/202503/understanding-the-results-of-dhs-sts-rivtd-biometrics-assessment#:~:text=found%20mdtf,and%20security; https://www.biometricupdate.com/202505/prevalence-of-fraud-as-a-service-models-eroding-online-trust-at-speed-jumio

[9] "The term PEP is commonly used in the financial industry to refer to foreign individuals who are or have been entrusted with a prominent public function, as well as to their immediate family members and close associates."; https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/20

d. Risk Assessment

i. Based on the information obtained, assigning a risk score that informs how the institution monitors a customer's activities.

10. KYC systems and rules are not designed or meant to be applied to software protocol intermediaries. As a consequence, KYC tools are created in a manner that renders them inapplicable to non-custodial software intermediaries such as Tornado Cash. In fact, there are multiple practical obstacles to Tornado Cash being able to implement and operate KYC tools on its software ecosystem that make their application impossible.

11. KYC tools are most often provided by third-party vendors that charge fees to provide KYC services. Those fees often range in the hundreds of thousands of dollars to operate. KYC service providers require contracts with a legal entity to perform services. The Tornado Cash structure, as an open-source software protocol (essentially just code), and not a company or organization with a defined structure, would likely preclude it from entering into the required contract with any KYC service providers.

12. When implementing a KYC tool, persons of sufficient expertise must conduct vendor due diligence on the tool and consider the possibilities of data security breaches, user privacy violations, operational disruptions, high false positive rates, and the potential for inaccurate data collection or verification.

13. Persons of sufficient expertise must also practically and routinely address system integration issues, address false-positive and name matches to KYC alerts, and map data elements between the KYC tool and applicable data systems. As software, Tornado Cash would have been incapable of:

a. Reviewing and investigating any alerts generated by the KYC tool due to lack of qualified staff and operating structure to review alerts;

b. Filing reports such as Suspicious Activity Reports (SARs) with FinCEN that are often triggered by KYC or other monitoring alerts due to lack of staff and operating structure to make professional adjudications of suspicious activity;

c. Discreetly filing reports such as SARs[10] that are required to be filed with FinCEN through the BSA e-filing system, the mandatory method of filing SARs[11] for obligated financial institutions;

d. Ensuring Tornado Cash users did not bypass attempts to enforce KYC protocols because the decentralized ecosystem could be accessed through previous versions of code;

e. Abiding by benchmarked model validation expectations as provided by the Office of the Comptroller of the Currency (OCC): *"Analysis of the integrity and applicability of internal and external information sources, including information provided by third-party vendors, should be performed regularly."*[12]

[10] FinCEN Mandatory E-Filing FAQs: "Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), Registration of Money Services Businesses (RMSBs), and Designation of Exempt Persons (DOEPs) must be E-Filed."
[11] https://www.fincen.gov/mandatory-e-filing-faqs
[12] OCC 2011-12: Supervisory Guidance On Model Risk Management, www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

f. Handling user complaints (legal or regulatory) related to data protection and data privacy issues as addressed by the Gramm-Leach-Bliley Act (GLBA) and the Federal Trade Commission (FTC).[13] The GLBA is a law that requires financial institutions to protect customers' sensitive data, to disclose how they share information, and limits when financial institutions can share nonpublic personal information with third-parties.

14. Yes, it is practically impossible or difficult to comply with the requirements but it would also pose ethical concerns. True financial institutions have agreements with customers and act as agents holding a position of trust vis a vis their customers. Software developers have no legal or ethical duty to act in the interests of their users. It would be therefore unethical to direct developers to collect, hold, and safeguard personal information about persons to whom they have no contractual relationship or duties.

15. Guidance from federal authorities illustrates the impossibility of Tornado Cash implementing proper KYC tools and processes in a reasonably safe or effective manner. For example, the Department of Justice notes in its guidance regarding third-party relationships (such as KYC vendors), that organizations should evaluate:

> "What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered[]"[14]

16. The U.S. government's "Interagency Guidance on Third-Party Relationships: Risk Management,"[15] while intended for banks, can also be used as a benchmark for the management of third-party vendors. The guidance notes specifically that sound third-party risk management includes:

> "Identifying and assessing the benefits and the risks associated with the business arrangement and determining how to appropriately manage the identified risks."[16]
>
> "Assessing a potential third-party's impact on customers, including access to or use of those customers' information, third-party interaction with customers, potential for consumer harm, and handling of customer complaints and inquiries."[17]
>
> "Understanding potential information security implications, including access to the banking organization's systems and to its confidential information."[18]

[13] https://www.ftc.gov/business-guidance/privacy-security
[14] www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline= , Page 8, Section E.
[15] A Notice by the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Comptroller of the Currency on 06/09/2023, https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management
[16] https://www.federalregister.gov/d/2023-12340/p-144
[17] https://www.federalregister.gov/d/2023-12340/p-150
[18] https://www.federalregister.gov/d/2023-12340/p-151

> "Determining how the…organization will select, assess, and oversee the third-party, including monitoring the third-party's compliance with applicable laws, regulations, and contractual provisions, and requiring remediation of compliance issues that may arise."[19]
>
> "Determining the… organization's ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis (including whether staffing levels and expertise, risk management and compliance management systems, organizational structure, policies and procedures, or internal control systems need to be adapted over time for the… organization to effectively address the business arrangement)."[20]

17. Neither code itself nor a decentralized community of software users are practically capable of making these evaluations or implementing appropriate controls over a third-party KYC tool because those activities require qualified people[21] to perform them. As a decentralized blockchain protocol, Tornado Cash did not possess - nor was it practically able to possess - the structure, staffing, or oversight by qualified persons to implement a third-party KYC system (or proprietary system) that would have:

    a. Met the intent of BSA and related KYC concepts;

    b. Enabled the confidential and technical requirements of the filing of SARs;

    c. Protected user data and information;

    d. Complied with regulatory guidance applicable to maintaining third-party vendor relationships and validate data and systems models; or

    e. Deterred users from using other variations of the code or user interface.

18. These are not automated, self-executing processes. Each requires a proactive team of professionals[22] that sets guidelines, reviews inputs, analyzes activity, performs investigations, and elevates reports. Qualified staff are needed to review and investigate any generated alert, investigate and write SARs and proactively file the reports through a secure server, and third-parties would need to conduct audits and analyses of the processes. As Tornado Cash operates simply as open-source software with no actual employees or owners, there is no one to perform any of these activities.

19. Werlau's suggestion that a "hypothetical smart contract could have been set up" "so that the Tornado Cash founders . . . had the ability to add or remove users based on a KYC process" reflects ignorance about how KYC processes are implemented, staffed, and managed. Any attempt to simply try to bolt a

[19] https://www.federalregister.gov/d/2023-12340/p-153

[20] https://www.federalregister.gov/d/2023-12340/p-154

[21] "*Human input and capacity building were identified as continuing to have an essential role in supporting the adoption of new technologies for AML/CFT, in particular regarding elements that technology still cannot overcome, regional inequalities or expertise on emerging issues.*"; Financial Action Task Force: OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT; 2021 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf

[22] "*The failure of an institution's leaders to devote sufficient staff to the BSA/AML compliance function may lead to other failures. For example, depository institutions, as well as other types of financial institutions, generally have staff that review alerts generated by transaction monitoring systems.*" FinCEN Advisory FIN-2014-A007; https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007#:~:text=The%20failure%20of%20an%20institution's,untimely%20reporting%20of%20suspicious%20activity.

third-party KYC solution onto a user interface without appropriate structure, evaluation, and operation would only create significant legal and operational risks for the software developers, and data security and data privacy risks for the users.[23]

OPINION 3: Due to inherent practical limitations in Automated Blockchain Monitoring (ABM) tools and processes, it was also impossible for Tornado Cash to apply ABM procedures.

20. ABM tools are software applications that continuously analyze blockchain data and automatically identify and flag potentially suspicious activity. These tools often use machine learning algorithms to detect unusual patterns and provide real-time and historical alerts. ABM alerts are *intended* to trigger a review of the related transactions and customer profile by qualified staff to determine whether or not the activity warrants reporting or other responses. Providers of common-use ABM tools include Elliptic, TRM, and Chainalysis. The Chainalysis ABM tool, called "Know-Your-Transaction" or KYT, is different from Chainalysis Sanctions Screening Oracle – a smart contract that checks if a cryptocurrency wallet address is on a sanctions list[24].

21. ABM tools are intended to provide an organization, in part, an understanding of the nature and purpose of transactions and conduct ongoing monitoring to identify and report suspicious transactions. ABM tools are limited in a variety of ways, and should not be viewed as a standalone system that makes an obligated organization "compliant" with the BSA without addressing those limitations.

22. ABM fundamentally and primarily relies on intelligence-based information gathered by third-party providers. It also differs in structure from "traditional" fiat transaction monitoring because it is not primarily based on mathematical patterns, thresholds, or time-bound movement of money. These intelligence-based alerts often present themselves weeks, months, or years after a transaction has actually taken place (ex post facto alerts), so an organization may often be unaware of any risk exposure at the time of the transaction.

23. It is common that an ABM-designated address was not attributable to illegal behavior at the time a user made a transfer. In cases where an ABM alert triggers long after a transaction and there was no other indicia of suspicion known at the time or reasonably thereafter, an organization must make risk-based decisions about whether a user knowingly engaged in illegal activity. This means trained personnel must analyze the relevant customer profile and comprehensive transaction activity.

24. ABM produces alerts for both direct and indirect transaction exposure to "risky"[25] addresses. The existence of either a direct or indirect alert does not inherently confirm that a transaction is part of an underlying crime.

25. Indirect transactions do not involve the direct transfer of funds between a wallet and an address designated by ABM as risky. Absent a reliable chain-of-custody analysis, each of the hops

[23] 16 CFR Part 314, "*The Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.*"; https://www.ftc.gov/legal-library/browse/rules/safeguards-rule

[24] https://www.chainalysis.com/free-cryptocurrency-sanctions-screening-tools/#sanctions-list

[25] In the context of Chainalysis, "risky" refers to cryptocurrency transactions or entities that exhibit characteristics or connections indicative of potential illicit activity, but not necessarily confirmed to be associated with illegal activity without more context.

(intermediaries) between a cryptocurrency wallet and the address associated with a "risky" address decreases the likelihood that the person making the transaction is knowingly engaged in criminal activity. Further, ABM alerts where a user's risk exposure is a minority percentage of the total transfer amount also indicates the likely actions of an unrelated third-party.

26. An organization may not be strictly obligated to treat the existence of an indirect transaction or an ex post facto alert, without more information, as indicative that a user has intentionally engaged in a transaction with a "risky" address, nor does a counterparty's ABM designation inherently suggest that a user is engaged in illegal activity. However, an organization and their qualified staff may monitor for composite behaviors that, even if resulting in indirect or ex post facto risk exposure, may indicate purposeful and coordinated avoidance of detection of suspicious activity.

27. Attributions by ABM tools themselves are also subject to flaws and inaccurate identification of addresses as "risky." ABM tools should not be exclusively relied upon to assess the risk designations of specific wallet addresses. While ABM tools are useful to implement a risk-based monitoring program, they are subject to error, and the assessment of whether a particular transaction or set of transactions is suspicious relies on the facts and circumstances of the transaction(s) as assessed by a trained compliance professional.

28. Neither code nor a decentralized community of software users are practically capable of operating a third-party ABM tool in the manner in which the ABM tools are designed. ABM tools require a robust effort by persons of sufficient expertise[26] to implement the tool's software into an organization's systems and data and operate on a routine basis.[27] Those tools require an organization's staff to map data elements between the ABM tool and the organization's data systems, to set and monitor ABM rule thresholds[28], to review and investigate alerts provided by the tool, and to escalate issues for possible reporting or other adverse action. Generally, the operation of ABM tools is conducted by persons of sufficient training and expertise in compliance matters. In fact, ABM vendors often require specific training by an organization's staff in order to operate the ABM tool.[29] Because neither the users of

[26] "The failure of an institution's leaders to devote sufficient staff to the BSA/AML compliance function may lead to other failures. For example, depository institutions, as well as other types of financial institutions, generally have staff that review alerts generated by transaction monitoring systems." FinCEN Advisory FIN-2014-A007; https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007#:~:text=The%20failure%20of%20an%20institution's,untimely%20reporting%20of%20suspicious%20activity.

[27] Chainalysis' KYT states that it permits users to "Manage alerts in bulk and collaborate via case management, enabling your team to quickly understand transactions that raise alerts, track statuses, conduct due diligence, and share insights to mitigate issues quickly." By its own terms, Chainalysis simply provides risk alerts that an entity's team then must mobilize to track and perform due diligence about.

[28] Risk-based transaction value, behavioral, and attributional thresholds.

[29] For example, the Chainalysis Reactor Certification (CRC) necessitates completion of CRC Training, which is intended for active Chainalysis Reactor users with prior experience and a foundational knowledge of bitcoin transactions. Similarly, Chainalysis' KYT requires staff to complete its KYT Essentials course, as noted in its prerequisites: "Participants must have completed our KYT Essentials course." Additionally, Elliptic Certify specifies that a "certificate [is] issued upon completion" of its training, indicating that staff must fully complete the program to be certified for its use. TRM Certified Investigator entails approximately 10 hours of training followed by a final assessment. These training prerequisites indicate that the effective use of such ABM tools generally relies on staff possessing specialized skills and knowledge.
https://www.chainalysis.com/chainalysis-reactor-certification/
https://academy.chainalysis.com/pages/ckc
https://www.elliptic.co/learn/certify
https://www.trmlabs.com/training-and-certifications/certified-investigator

Tornado Cash nor the protocol itself would possess the training, expertise, authority, and responsibility to operate an ABM tool, there is likely no practical way for the ABM tool to have been utilized to meet its intended use of identifying, investigating, confirming, or reporting illicit activity.

29. Even if Tornado Cash was able to overcome the significant limitations to implement an ABM tool, as software, the protocol itself would still have been incapable of:

    a. Adjusting ABM thresholds and detection settings;

    b. Reviewing and investigating any alerts generated by the ABM tool due to lack of qualified staff and operating structure to review alerts;

    c. Discreetly adjudicating the need for, then filing reports such as SARs[30] that are required to be filed through the BSA e-filing system, the mandatory method of filing SARs[31] for obligated financial institutions;

    d. Abiding by benchmarked model validation expectations as provided by the OCC: "Analysis of the integrity and applicability of internal and external information sources, including information provided by third-party vendors, should be performed regularly."[32]

30. These are not automated, self-executing processes. Instead, they require a proactive team of professionals[33] that set guidelines, review inputs, analyze activity, perform investigations, and write and file reports. As Tornado cash is simply open-source software with no actual employees or owners, there is no one to perform any of these activities.

31. The Department of Justice notes in its guidance regarding third-party relationships (such as ABM vendors), that organizations should evaluate, "[w]hat mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered[.]"[34]

32. The U.S. government's "Interagency Guidance on Third-Party Relationships: Risk Management,"[35] while intended for banks, can be used as a benchmark for the management of third-party vendors. As

---

[30] FinCEN Mandatory E-Filing FAQs: "Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), Registration of Money Services Businesses (RMSBs), and Designation of Exempt Persons (DOEPs) must be E-Filed."
[31] https://www.fincen.gov/mandatory-e-filing-faqs
[32] OCC 2011-12: Supervisory Guidance On Model Risk Management, www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf
[33] "The use of new technologies for monitoring purposes should, for the most part, continue to be integrated with the broader monitoring systems which include an element of human analysis for specific alerts or areas of higher risk. These systems must also improve their degree of explainability and auditability in order to fully comply with the majority of supervisory requirements." Financial Action Task Force: OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT; 2021; https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf
[34] www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline= , Page 8, Section E.
[35] A Notice by the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Comptroller of the Currency on 06/09/2023, https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management

detailed herein under Opinion 2 in Section 6, there are a number of evaluations expected from financial institutions and money transmitters when engaging with third-party vendors. Neither code nor a decentralized community of software users are practically capable of making these evaluations or implementing appropriate controls over a third-party ABM tool because those activities require qualified people, not code, to perform them in a manner that would meet regulatory expectations. Even the most basic of recommended actions could not be accomplished. Since Tornado Cash is essentially just code, and not a company with a defined ownership structure, there is no ability to enter into the contract required by most KYC service providers. Software cannot be a counterparty to a contract.

33. In sum, Tornado Cash, as software, could not possess the structure, staffing, or oversight to be able to practically or appropriately operate an ABM system or report results of ABM monitoring outcomes through reporting mechanisms provided by FinCEN. As such, abiding by related monitoring and illicit activity reporting expectations was an actual impossibility.

OPINION 4: Transactions that possess privacy features either by intent or technical application should not be viewed as inherently illicit.

34. Portions of the government's experts' disclosed opinions imply that transactions that are anonymous or private are inherently illicit. However, from a compliance standpoint, the use of VPNs, relayers, or other anonymizing techniques by users of Tornado Cash does not signal that the digital assets interacting with the Tornado Cash protocol were derived from illegal activity absent other risk indicators.

35. Traditional financial transactions are not public and can only be obtained from financial institutions in controlled environments such as legal orders, information sharing provisions with legal safe-harbor provisions[36], or established regulatory reporting frameworks making them inherently more private

36. Public blockchains, however, expose transaction details, an inherent privacy weakness. Each transaction on the blockchain is recorded with a public key, which may not directly reveal the identity of the user but can be traced. Over time, with enough data and analysis, these public keys can be linked to real-world identities:

    a. Public keys are unique identifiers for cryptocurrency wallets.

    b. Transactions are recorded on a public ledger that anyone can access.

    c. Identifying patterns in transactions can lead to uncovering real identities.

37. Because public blockchain transactions possess a higher level of public transparency than traditional financial transactions, a blockchain system absent that same level of public transparency, which seeks to restore some of the privacy afforded to traditional financial transactions should not be considered inherently illicit in and of itself.

[36] Such as FinCEN's 314(a) and 314(b) programs.

38. Privacy-enhancing features and tools are a critical component to digital safety[37] and are both used and encouraged by government entities, financial institutions, and individuals in order to protect personal assets and information.

39. There are a variety of valid reasons that any person or organization would be interested in protecting the privacy of their digital transactions and identities:

    a. Sensitive data transmitted over unsecured networks, such as public Wi-Fi, risks interception by attackers.

    b. Anonymity can limit phishing, social engineering, and targeted cyberattacks by concealing transactional metadata and user identities.

    c. Businesses often handle proprietary data or confidential transactional information (e.g., M&A, strategic partnerships) where discretion is critical.

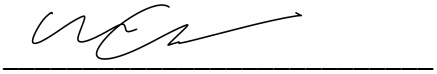
    d. Digital transactions often contain sensitive personal information (e.g., name, address, payment details) that can be exploited if intercepted or leaked.

40. Various government and regulatory agencies acknowledge VPNs as secure communication mechanisms, protecting data in transit. The FTC reinforces this by urging scrutiny of VPN providers, affirming their role in mitigating risks of exposure on public networks. VPNs, endorsed by the FBI and FTC as part of cybersecurity hygiene, encrypt data and conceal origins, reducing exposure to theft or misuse, as highlighted in the Protected Voices initiative.

41. In sum, transactions and digital activities that possess privacy features either by intent, technical application, or use of third-party tools such as VPNs should not be viewed as inherently illicit. Rather, privacy tools are an important element of routine digital and financial safety measures commonly used by the public and varyingly acknowledged and encouraged by government agencies.

Approval and Signature

I approve the disclosure of my qualifications, opinions, and bases for such opinions, as set forth above.



Michael J. Carter

[37] Does Crypto Make You a Target? Emerging Physical Risks of Digital Wealth; https://www.globalguardian.com/global-digest/crypto-physical-risks